APPLICATION FOR UNITED STATES PATENT

by

RAYMOND JAY HARPER

and

DANIEL DOUTT

for

METHODS AND SYSTEMS FOR NETWORK ELEMENT FAULT INFORMATION PROCESSING

SHAW PITTMAN LLP
1650 Tysons Blvd., 14th Floor
McLean, Virginia 22102-4859
(703) 770-7900

Attorney Docket No.: BS01-327

METHODS AND SYSTEMS FOR
NETWORK ELEMENT FAULT INFORMATION PROCESSING

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] Embodiments of the present invention relate to network communications systems. More particularly, embodiments of the present invention relate to systems and methods for network element fault information processing.

BACKGROUND INFORMATION

[0002] A known telecommunications management system is the NavisCore™ Element Management System from Lucent Technologies of Murray Hill, New Jersey. NavisCore is a centralized service and network management application. It can provide standards-based management and control of telecommunications network elements of networks such as frame relay, Switched Multimegabit Data Service ("SMDS"), Asynchronous Transfer Mode ("ATM"), and Internet Protocol ("IP") switch networks. NavisCore includes a distributed and multiservice element manager and is a graphically integrated UNIX-based platform that provides a network management solution based on Telecommunications Network Management ("TNM") standards.

[0003] NavisCore can speed circuit provisioning with point-and-click operations to establish end-to-end network connectivity and provides a variety of traps for alarm indications and statistics logic for elements in the switch network such as switches, trunks, physical ports, logical ports, permanent virtual circuits ("PVCs"), switched virtual circuits, and so on. A NavisCore user can use network statistics for real-time status information on logical and physical ports and view key usage data on such interfaces for network planning and trend analysis. Network element faults (i.e., network faults) can be reported to a central repository where a NavisCore operator can access the network element fault information.

[0004] A central repository receiving the reported network element faults is typically one or more NavisCore servers. The NavisCore servers record the reported element network faults in files typically called trap logs. Examples of trap log information are as follows:

985885337 1 Thu Mar 29 12:02:17 2001 NWORLAMABB1 - Switch nworlamabb1 interface up (SNMP linkUp trap) on LPort 60QGDA500180 _LMC(14,7);1.1.3.6.1.4.1.277.10.0.10003 0;

985885337 7 Thu Mar 29 12:02:17 2001 NWORLAMABB1 - LPort 60QGDA500180_LMC(14,7) at switch nworlamabb1 is up with Customer Name SUPERS_SUPERMARKET.;3 .1.3.6.1.4.1.277.10.0.30 0;

and

985885533 7 Thu Mar 29 12:05:33 2001 NWORLAMABB1 - LPort 60QGDA500180_LMC(14,7) in switch nworlamabb1 is up, following PVCs is also up: HOUM_SUPERS_SUPERMARKE_100_99 NWOR_SUPERS_SUPERMARK ET_100_101 NWOR_SUPERS_SUPERMARKET_100_103 NWOR_SUPERS_SU PERMARKET_100_104 NWOR_SUPERS_SUPERMARKET_100_105 NWOR_R OUSES_SUPERMARKET_100_106 NOWR_SUPERS_SUPERMARKET_100_107 NWOR_SUPERS_SUPERMAR

KET_100_108 NWOR_SUPERS_SUPERMARKE T_100_109 NWOR_SUPERS_SUPERMARKET_110_110 NWOR_SUPERS_MR KT_NNI_BTR_202_758 HOUM_SUPERS_SUPERMARKET_203_203 .;1 .1.3.6.1.4.1.277.10.0.10009.

[0005] Trap logs and other network element fault information can indicate network fault events but are cumbersome to search and display. For example, if a customer of a network services provider complains about service problems (e.g., loss of service, degrading of service levels, and so on) a network technician can retrieve and sequentially review the trap logs to determine information about the customer's network services. In view of the foregoing, it can be appreciated that a substantial need exists for systems and methods that can advantageously provide for network element fault information processing.

BRIEF SUMMARY OF THE INVENTION

[0006] Embodiments of the present invention relate to systems and methods for network element fault information processing. In an embodiment, a network element identifier and a network element fault information processing instruction are received. A query for network element fault information based at least in part on the network element identifier is sent. Network element fault information is received. The network element fault information is processed based at least in part on the received network element fault instruction. The processed network element fault information is output.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 is a schematic diagram of an embodiment of the present invention.

[0008] Figure 2 illustrates a system in accordance with an embodiment of the present invention.

[0009] Figure 3 illustrates a method in accordance with an embodiment of the present invention.

[0010] Figure 4 shows an example of processed network element fault information in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] According to an embodiment of the present invention, a system receives an instruction (e.g., from a user) to retrieve network element fault information from a server that stores, for example, network fault information corresponding to a network element. For example, the server can be coupled to one or more network elements such as a network switch, a network circuit, a network path, and so on. When a network fault related to a network element is detected, information corresponding to the network fault can be sent to the server for storage in a trap log. The network element fault information can include, for example, an identifier of the network element, a fault type identifier corresponding to the type of network fault, a time and/or date identifier associated with the time and/or date of the network fault, and so on.

[0012] The instruction to retrieve network element fault information corresponding to a network element can include a network element identifier corresponding to the network element. For example, a user can input a network element identifier, and the network element identifier can be a permanent virtual circuit ("PVC") identifier, a logical port ("LP") identifier, and so on. One or more trap logs corresponding to the network element can be queried for and received. The instruction to retrieve the trap log information can also include a requested fault type identifier that specifies which type of fault type information should be output (e.g., displayed, printed, etc.) to the user. For example, a user may be interested in displaying network fault information associated with network element transitions to an up state. The trap log can be analyzed (e.g., searched, parsed, etc.) to determine network fault information associated with the requested fault type identifier, and the determined network fault information can be presented to the user.

[0013] Figure 1 is a schematic diagram of an embodiment of the present invention. Network 101 includes interior switches 110, 111, 112, and 113 (e.g., core switches, etc.), which are coupled together. As used to describe embodiments of the present invention, the term "coupled" encompasses a direct connection, an indirect connection, or a combination thereof. Moreover, two devices that are coupled can engage in direct communications, in indirect communications, or a combination thereof. Network 101 can be a data network such as a frame relay network, an SMDS network, an ATM network, an IP network, a Multiprotocol Label Switching ("MPLS") network, an X.25 network, and so on. Accordingly, switches 110-113 can be frame relay switches, SMDS switches, ATM switches, IP switches, MPLS switches, X.25 switches, and so on.

[0014] Network 101 can also include switches such as an edge switch 120, which is coupled to one or more interior switches such as, for example, interior switches 111 and 113. An edge switch 120 is typically the first point of user (e.g., customer) access to a network and the final point of exit for communications to the user. Edge switches are typically inter-coupled by interior switches such as switches 110-113.

Edge switch 120 is coupled to customer premises equipment 165 of a customer location 160 via a communications link 166. Examples of customer premises equipment 165 include a switch, a router, a network interface device, a modem, a cable modem, a digital subscriber line ("DSL") modem, and so on. Examples of communications link 166 include a 56K line, a 64K line, a T1 connection, a T3 connection, and so on. Further examples of communications link 166 include a PVC, a permanent virtual path ("PVP"), and so on. In an embodiment, communications link 166 is associated with a logical port.

[0015] Figure 2 illustrates a system in accordance with an embodiment of the present invention. Network faults can occur with respect to communications between edge switch 120 and CPE 165 via communications link 166. For example, communications to and/or from edge switch 120 can bounce, the communications link 166 can go down and subsequently up, CPE 165 may not function properly, and so on. In an embodiment in which network 101 of Figure 1 is a frame relay network, frame errors can occur. In an embodiment in which network 101 is, for example, an ATM network or a frame relay network, communications link 166 can be a PVC or PVP that goes down periodically. In a further embodiment, communications link 166 can include one or more communication sub-links 167 (e.g., cables, wires, optical fibers, circuits, etc.) and/or associated equipment such as amplifiers, multiplexers ("MUXs"), and so on. A network fault can be a faulty amplifier, a failed MUX, a short circuit, and so on. Based in part on the description of embodiments of the present invention provided herein, other examples of network faults will be apparent to one of skill in the art.

[0016] Edge switch 120 can determine network faults corresponding to edge switch 120, communications link 166, and/or CPE 165 and report the network faults to server 150. For example, edge switch 120 can send a network fault report (e.g., a network fault message) to server 150 after determining one or more network faults. Edge switch 120 can include parameters that can determine at least in part when network fault conditions are to be reported to server 150. For example, edge switch 120 can include parameters that establish that certain types of network faults (e.g., frame errors, down errors, etc.) are reported to server 150. Edge switch 120 can also include parameters that establish a threshold severity or persistence of a network fault that will result in reporting the network fault to server 150. For example, a down error can be reported to server 150 when it lasts more than five (5) cycles. Alternatively, individual frame errors may not be reported to server 150, but after a threshold value related to frame errors is met or exceeded, a frame error network fault report can be sent to server 150. For example, a certain number of frame errors in a period of time can trigger sending of a frame error network fault report to server 150.

[0017] Server 150 can store received network fault reports received from edge switch 120. For example, server 150 can store network fault reports received from edge switch 120 in a directory where each network fault report identifies a type of network fault, a date and/or time associated with the network fault, a network element associated with the network fault, and so on. In another embodiment, server 150 can store network fault reports received from edge switch 120 in a network fault report file where corresponding network fault reports are stored so that the network fault report file includes a history of network fault reports. In an embodiment, the network fault report file includes network fault reports from a long-term period (e.g., days, weeks, months, years, etc.). In another embodiment, the network fault report file is a buffer file that includes network fault reports for a rolling period of time (e.g., the previous five hours, the previous four days, the previous week, the previous 30 days, and so).

[0018] In an embodiment of the present invention, server 150 can be coupled to edge switch 120 via interior switch 113 and communication paths 221 and 222. In another embodiment, server 150 can be coupled to edge switch 120 via a communications path 226. Server 150, in an embodiment, can be a NavisCore server that receives network management information from edge switch 120. According to an embodiment, edge switch 120 includes a trap, which is a mechanism permitting a device to send (e.g., automatically, autonomously, periodically, etc.) an alarm for certain network events to a management station. Typically, network management information is acquired by polling network nodes on a periodic (e.g., regular) basis, but such a network management information acquisition strategy can be modified when a trap is set from a network device. With traps, a network element (e.g., a network node) alerts the management of an event (e.g., a network fault, a routine event, a catastrophic event, etc). The management station, in an embodiment, can initiate a polling sequence to network elements (e.g., nodes) to determine potential causes of the event. Such a trap and poll strategy is often called trap-directed polling.

[0019] Network management personnel often become aware of network faults when a customer (e.g., an owner or operator of CPE 165) complains that its communications are degraded or inoperative. To diagnose why the customer communications are degraded or inoperative, network management personnel often examine network fault reports stored on server. For example, network management personnel can examine network fault information stored on server 150 to ascertain whether there are any network faults associated with communications link 166, edge switch 120, and/or CPE 165.

[0020] Known methods of analyzing the network fault information relate to examining the native (e.g., unprocessed) network fault reports stored on server 150. For example, a network management technician can examine individual network fault reports (e.g., trap logs stored on a server) such as the following:

985885337 1 Thu Mar 29 12:02:17 2001 NWORLAMABB1 - Switch nworlamabb1 interface up (SNMP linkUp trap) on LPort 60QGDA500180 _LMC(14,7);1.1.3.6.1.4.1.277.10.0.10003 0;

985885337 7 Thu Mar 29 12:02:17 2001 NWORLAMABB1 - LPort 60QGDA500180_LMC(14,7) at switch nworlamabb1 is up with Customer Name SUPERS_SUPERMARKET.;3 .1.3.6.1.4.1.277.10.0.30 0;

and

985885533 7 Thu Mar 29 12:05:33 2001 NWORLAMABB1 - LPort 60QGDA500180_LMC(14,7) in switch nworlamabb1 is up, following PVCs is also up: HOUM_SUPERS_SUPERMARKE_100_99 NWOR_SUPERS_SUPERMARK ET_100_101 NWOR_SUPERS_SUPERMARKET_100_103 NWOR_SUPERS_SU PERMARKET_100_104 NWOR_SUPERS_SUPERMARKET_100_105 NWOR_R OUSES_SUPERMARKET_100_106 NOWR_SUPERS_SUPERMARKET_100_107 NWOR_SUPERS_SUPERMAR

KET_100_108 NWOR_SUPERS_SUPERMARKE T_100_109 NWOR_SUPERS_SUPERMARKET_110_110 NWOR_SUPERS_MR KT_NNI_BTR_202_758 HOUM_SUPERS_SUPERMARKET_203_203 .;1 .1.3.6.1.4.1.277.10.0.10009.

[0021] Native network fault information, such as the examples above, are difficult to review and analyze. The native network fault information provides required information, but also can include too much information when attempting to troubleshoot a fault or problem in a communications network. In an embodiment of the present invention, network fault information is identified, retrieved, and processed to aid in network management analysis and operations. For example, a network element can be identified, a network fault type can be specified, network element fault information associated with the network element can be retrieved, and the network fault information can be processed based in part on the specified network fault type.

[0022] Figure 3 illustrates a method in accordance with an embodiment of the present invention. A user can be prompted to enter a network element identifier (step 305). For example, a network element identifier can be a switch identifier, a circuit identifier, a communications link identifier, a PVC identifier, a logical port identifier, a combination thereof, and so on. In an embodiment, a user can be prompted to enter one or more network element identifiers such as a switch identifier and a circuit identifier. In another embodiment, a user can be prompted to enter a trap log identifier, a NavisCore server identifier, a combination thereof, and so on. In an embodiment, the user is prompted to enter a network element identifier by a computer program or a software script executing on a computer.

[0023] For example, referring again to Figure 2, a computer 290 can be coupled to server 150. In an embodiment, computer 290 includes a processor and a memory. The processor can be, for example, an Intel Pentium® 4 processor, manufactured by Intel Corp. of Santa Clara, California. As another example, the processor can be an Application Specific Integrated Circuit (ASIC). The memory may be a random access memory (RAM), a dynamic RAM (DRAM), a static RAM (SRAM), a volatile memory, a non-volatile memory, a flash RAM, polymer ferroelectric RAM, Ovonics Unified Memory, magnetic RAM, a cache memory, a hard disk drive, a magnetic storage device, an optical storage device, a magneto-optical storage device, or a combination thereof. The memory of computer 290 can store a plurality of instructions adapted to be executed by processor of computer 290.

[0024] In an embodiment, computer 290 is coupled to server 150 via a network 295 and a network connection (e.g., data port, input/output port, etc.). Examples of a network 295 include a Wide Area Network (WAN), a Local Area Network (LAN), the Internet, a wireless network, a wired network, a connection-oriented network, a packet network, an Internet Protocol (IP) network, or a combination thereof.

[0025] Referring again to Figure 3, a network element identifier can be received (step 310). The user can be prompted to enter a network element fault information processing instruction (step 315). For example, a network element fault information processing instruction can be an instruction to display transitions to a down state, an instruction to display transitions to an up state, an instruction to display a log of transitions for a period of time (e.g., the previous day, the previous four days, the previous week, etc.), an instruction to display network element fault information in a simplified format, an instruction to display network element fault information in the native format, a combination thereof, and so on. The network element fault information processing instruction can be received (step 320). Based at least in part on the received network element identifier, network element fault information corresponding to the network element identified by the network element identifier can be received. For example, the network element fault information can be queried for from a NavisCore server associated the identified network element. In another embodiment of the present invention, the network element fault information is queried from the network element. In a further embodiment of the present invention, the identified network element receives the query for the network element fault information and sends the query to a network management station (e.g., a server) that receives network fault information from the network element.

[0026] After the network element fault information is received, it can be processed based at least in part on the received network element fault information processing instruction (step 330). For example, when the received network element fault information processing instruction is an instruction to display transitions to an up state, the network element fault information can be processed to isolate and/or summarize the network fault information corresponding to transitions to an up state. As another example, when the received network element fault information processing instruction is an instruction to display transitions to a down state, the network element fault information can be processed to isolate and/or summarize the network fault information corresponding to transitions to a down state. In another example, when the received network element fault information processing instruction is an instruction to display a log of transitions for a period of time, the network element fault information can be processed to isolate and/or summarize the network element fault information corresponding to transitions to an up state and transitions to a down state. After the received network element fault information has been processed based at least in part on the received network element fault information processing instruction, the processed network element fault information can be output (step 335). For example, the processed network element fault information can be output to a printer, to a display device (e.g., a Cathode Ray Terminal ("CRT") display, a Liquid Crystal Diode ("LCD") display, a video display, a text display, a dumb terminal, etc.), to a personal digital assistant ("PDA"), to a combination thereof, and so on.

[0027] Figure 4 shows an example of processed network element fault information in accordance with an embodiment of the present invention. A user can specify a network element identifier and a network element fault information processing instruction. Network element fault information corresponding to the network element identifier can be queried for and received, and then processed based at least in part on the network element fault information processing instruction. For example, a user can specify that information about specific types of network element faults for a network element be identified and summarized.

[0028] In an embodiment of the present invention, a data record 400 is generated based on a specified processing of network element fault information. Data record 400 can correspond to a network element such as a network switch, a network circuit, a network logical port, a combination thereof, and so on. Data record 400 can include one or more entries 410, and each entry of at least a subset of the one or more entries 410 can include one or more chronological data fields to store chronological data. For example, data record 400 can include an entry 410 including a month identifier field 411 to store a month identifier and a date identifier field 412 to store a date identifier. Entry 410 of data record 400 can also include one or more network fault indicator fields. For example, entry 410 can include a down state field 413 to store a down state value (e.g., a number of times a network element was in a down state, a boolean value indicating whether the network was in a down state, etc.), an up state field 414 to store an up state value, a frame error state field 415 to store a frame error state value, and a remainder network fault state field 416 to store a remainder network fault state value.

[0029] For example, data record 400 is generated based at least in part on native network fault information received from a network management station (e.g., trap log information from a NavisCore server). The native network fault information is processed to identify and/or summarized network faults. Data record 400 indicates, for example, that the network element corresponding to data record 400 reported the following number of down network faults for March 26 through March 30 respectively: 0, 18, 122, 106, and 94. The network element also reported the following number of up network faults for March 26 through March 30 respectively: 0, 20, 86, 132, and 144. The network element did not report any frame errors or any remainder network faults for March 26 through March 30. According to alternative embodiments of the present invention, a data record can be generated that includes processed network element fault information corresponding to one or more network faults over varying periods of time (e.g., day by day, hour by hour, week by week, minute by minute, and so on).

[0030] Embodiments of the present invention relate to data communications via one or more networks. The data communications can be carried by one or more communications channels of the one or more networks. A network can include wired communication links (e.g., coaxial cable, copper wires, optical fibers, a combination thereof, and so on), wireless communication links (e.g., satellite communication links, terrestrial wireless communication links, satellite-to-terrestrial communication links, a combination thereof, and so on), or a combination thereof. A communications link can include one or more communications channels, where a communications channel carries communications. For example, a communications link can include multiplexed communications channels, such as time division multiplexing ("TDM") channels, frequency division multiplexing ("FDM") channels, code division multiplexing ("CDM") channels, wave division multiplexing ("WDM") channels, a combination thereof, and so on.

[0031] In accordance with an embodiment of the present invention, instructions adapted to be executed by a processor to perform a method are stored on a computer-readable medium. The computer-readable medium can be a device that stores digital information. For example, a computer-readable medium includes a compact disc read-only memory (CD-ROM) as is known in the art for storing software. The computer-readable medium is accessed by a processor suitable for executing instructions adapted to be executed. The terms "instructions adapted to be executed" and “instructions to be executed” are meant to encompass any instructions that are ready to be executed in their present form (e.g., machine code) by a processor, or require further manipulation (e.g., compilation, decryption, or provided with an access code, etc.) to be ready to be executed by a processor.

[0032] Systems and methods in accordance with an embodiment of the present invention disclosed herein can advantageously process (e.g., analyze and/or summarize) network element fault information. A user can identifier a network element by inputting one or more network element identifiers. The user can also specify a network element fault information processing instruction. The network element fault information can be processed based at least in part on the specified network element fault information processing instruction.

[0033] Embodiments of systems and methods for network element fault information processing have been described. In the foregoing description, for purposes of explanation, numerous specific details are set forth to provide a thorough understanding of the present invention. It will be appreciated, however, by one skilled in the art that the present invention may be practiced without these specific details. In other instances, structures and devices are shown in block diagram form. Furthermore, one skilled in the art can readily appreciate that the specific sequences in which methods are presented and performed are illustrative and it is contemplated that the sequences can be varied and still remain within the spirit and scope of the present invention.

[0034] In the foregoing detailed description, systems and methods in accordance with embodiments of the present invention have been described with reference to specific exemplary embodiments. Accordingly, the present specification and figures are to be regarded as illustrative rather than restrictive.